Security Architecture Work Group

Monday May 14, 2001
1:30 p.m. to 3:00 p.m.
Executive Building Video Conference Room
521 South 14th Street,
Lincoln, Nebraska

Minutes

A. Participants

Allan	Albers	HHSS/IS&T
Jason	Everett	ESU 10
Margo	Gamet	HHS
Jerry	Hielen	IMServices
Sandy	LaLonde	IMServices
Dennis	Linster	Wayne State College
Scott	McFall	State Patrol
George	McMullin	Nebraska CERT / USSTRATCOM
Leona	Roach	University of Nebraska Computing Services Network
Steve	Schafer	Nebraska CIO

1) Security web site (http://www.nitc.state.ne.us/tp/workgroups/security/index.htm)

Steve Schafer invited comments and suggestions regarding the security web site.

2) Security Procedures Documentation

Jerry Hielen introduced Sandy LeLonde who is working on the documentation of procedures. Jerry and Sandy gave a presentation that summarized their approach. The purpose of the project is to provide a structure that will enable agencies to develop a comprehensive information security program. Aspects will include blueprints for the security manager, guides for developing procedures, and the outline for an awareness program. Besides IMServices, the project team includes HHSS, DOR, UN, and ESU 10. They plan to make maximum use of any existing materials and resources.

Deliverables will include:

a) Templates for the security professional who is developing a comprehensive information security program;
b) Templates for preparing an information security handbook and an awareness program for non-IT employees;
c) Change control process for maintaining and updating security documentation;

The documents will emphasize self-teaching, using a fill-in the blank process. The templates will not be limited to a specific technology or agency. The security templates will promote HIPAA compliance and conform to the NITC security policies. They will include checklists, glossaries, and a format for organization and presentation. There will be step-by-step instructions for completing each template.

Developing the templates will involve six tasks:

a) Requirements definition
b) Design and organization
c) Create prototype

d) Gathering information / development
e) Testing/review/editing
f) Implementation

The timeline calls for a prototype to be done by May 30, a first draft by June 19, and the final product by June 30.

Discussion included the following suggestions:

a) The agency level comprehensive information technology plans should reinforce the requirement for security planning
b) OMB Circular A130 is a potential resource
c) An effective awareness program is key to success. For example Stratcom mandates periodic training, including computer-based training on new items and issues and refresher training
d) Legal liability was a major motivator for executive interest in Year 2000. HIPAA and other federal legislation relating to financial privacy is now creating a similar environment where liability for privacy and security failures will affect high level management.
e) Bugtraq of security focus.com is another resource.

2) Discussion of Incident Reporting Policy for state agencies

Steve Schafer asked for opinions regarding an incident reporting process for state agencies. He cited concerns about the number of agencies affected by recent attacks on web sites. Presently, no one knows the true extent or severity of the problem. Comments included:

a) It will be important to minimize the impact of any reporting system on agencies, otherwise few will comply;
b) Agencies must be able to understand the purpose of reporting incidents and see some benefit to themselves;
c) Tracking incidents is important in order to establish patterns, share information about vulnerabilities, and developing a business case for more attention to security issues;
d) The University found that reporting incidents was essential to gaining attention of administrators. The University now has a well-developed incident reporting process.
e) Wayne State College ceased reporting incidents to law enforcement or national organizations, because there was never any follow-up.

Discussion did not produce a clear direction on this issue, other than agreement that it is easier for people to react to a sample process than to develop one from scratch at a meeting.

3) Other Implementation Options

a. Business Case Outline
b. CERT Conference -- August 6 to 10
c. Fall Security Technical Forum (early November?)
d. Templates for Security Plans and Programs

4) Other Options

5) Next Meeting Date

The next meeting is Monday June 11 at 1:30, same locations.